AO 106 (Rev. 04/10) Application for a Search Warrant

HH

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
All Meet24 accounts associated with Registration IP Address 65.24.236.92

Case No. 2:20-mj-337

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A, incorporated herein by reference

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment B, incorporated herein by reference

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more):*

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2251	Production/advertising for child pornography in interstate commerce
18 USC 2422(b)	Coercion/enticement of a minor in interstate commerce
18 U.S.C. 2252/2252A	Receipt, distribution, and/or possession of visual depictions of a minor engaged in sexually explicit conduct and/or child pornography, in interstate commerce

The application is based on these facts:

See attached affidavit incorporated herein by reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Josh Saltar, SA FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: May 8, 2020

City and state: Columbus, Ohio

Elizabeth A. Preston Deavers
United States Magistrate Judge

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT, WESTERN DIVISION OF OHIO

In the Matter of the Search of:	)	**Case No:**
	)	**Magistrate Judge**
All Meet24 accounts associated with	)	
Registration IP Address 65.24.236.92	)	
	)	

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Josh Saltar ("your affiant"), a Special Agent (SA) with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state:

I. EDUCATION TRAINING AND EXPERIENCE

1. I am a SA with the FBI and have been since October 2014. I am currently assigned to the Cincinnati Field Office, Violent Crimes Against Children Squad investigating matters involving the online exploitation of children and child pornography, and I am trained and authorized to investigate the offenses alleged herein.

2. During my career as a SA, I have participated in various investigations involving computer-related offenses and have executed numerous search warrants, including those involving searches and seizures of computers, digital media, software, and electronically stored information. I have received both formal and informal training in the detection and investigation of computer-related offenses involving children. I have also received formal training from industry leading forensic examiners and cyber incident responders. As part of my duties as a SA, I investigate criminal child exploitation and child pornography violations, including the illegal production, distribution, transmission, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252(a) and 2252A.

3. As a SA with the FBI, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

II. PURPOSE OF THE AFFIDAVIT

4. The facts set forth below are based upon my own personal observations, investigative reports, and information provided to me by other law enforcement agents. I have not included in this affidavit all information known by me relating to the investigation. I have set forth only the facts believed to be necessary to establish probable cause for a search warrant for the Meet24 accounts associated with Registration IP Address 65.24.236.92 (hereinafter the "**ACCOUNTS**"). I have not withheld any evidence or information which would negate probable cause.

5. The **ACCOUNTS** to be searched is more particularly described in Attachment A, for the items specified in Attachment B, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2251, 2252 and 2252A – the production, advertising of/for, distribution, transmission, receipt, and/or possession of child pornography and 2422(b) – Coercion or Enticement of a Minor to Engage in Illegal Sexual Activity.

III. APPLICABLE STATUTES AND DEFINITIONS

6. Title 18 United States Code, Section 2251(a) makes it a federal crime for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in, or have a minor assist any other person to engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that either the visual depiction will be transported or transmitted via a facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or that the visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce, or if the visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce. Subsection (e) of this provision further prohibits conspiracies or attempts to engage in such acts.

7. Title 18 United States Code, Section 2251(d)(1)(A) makes it a federal crime for any person to make, print, publish, or cause to be made, printed or published, any notice or advertisement that seeks or offers to receive, exchange, buy, produce, display, distribute or reproduce, any visual depiction involving the use of a minor engaging in sexually explicit conduct, if such person knows or has reason to know that either the notice or advertisement will be transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mail; or that the notice or advertisement actually was transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mail.

8. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce, or is in or affecting interstate commerce.

9. Title 18, United States Code, Section 2252A, makes it a federal crime for any person to knowingly transport, receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.

10. Title 18, United States Code, Section 2422(b) makes it a federal crime for any person to knowingly use a means of interstate commerce to persuade, induce, entice, or coerce or attempt to persuade, induce, entice or coerce, any individual who has not attained the age of 18 years, to engage in any sexual activity for which any person may be charged with a crime, including the production of child pornography as defined in 18 U.S.C. §§ 2251(a) and 2256(8).

11. As it used in 18 U.S.C. §§ 2251 and 2252, the term "sexually explicit conduct" is defined in 18 U.S.C. § 2256(2) (A) as: actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person.

12. As it is used in 18 U.S.C. § 2252A(a)(2), the term "child pornography"[1] is defined in 18 U.S.C. § 2256(8) as: any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual

1 The term child pornography is used throughout this affidavit. All references to this term in this affidavit and Attachments A and B hereto, include both visual depictions of minors engaged in sexually explicit conduct as referenced in 18 U.S.C. § 2252 and child pornography as defined in 18 U.S.C. § 2256(8).

depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

13. The term "sexually explicit conduct" has the same meaning in § 2252A as in § 2252, except that for the definition of child pornography contained in § 2256(8)(B), "sexually explicit conduct" also has the meaning contained in § 2256(2)(B): (a) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (b) graphic or lascivious simulated; (i) bestiality; (ii) masturbation; (iii) sadistic or masochistic abuse; or (c) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.

14. The term "minor", as used herein, is defined pursuant to Title 18, U.S.C. § 2256(1) as "any person under the age of eighteen years."

15. The term "graphic," as used in the definition of sexually explicit conduct contained in 18 U.S.C. § 2256(2)(B), is defined pursuant to 18 U.S.C. § 2256(10) to mean "that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted."

16. The term "visual depiction," as used herein, is defined pursuant to Title 18 U.S.C. § 2256(5) to "include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image."

17. The term "computer"[2] is defined in Title 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

IV. BACKGROUND REGARDING COMPUTERS, DIGITAL STORAGE DEVICES, THE INTERNET AND MOBILE APPLICATIONS

18. Computers, mobile devices and the Internet have revolutionized the ways in which those

[2] The term "computer" is used throughout this affidavit to refer not only to traditional laptop and desktop computers, but also to internet-capable devices such as cellular phones and tablets. Where the capabilities of these devices differ from that of a traditional computer, they are discussed separately and distinctly.

with a sexual interest in children interact with each other and with children they seek to exploit. These new technologies have provided ever-changing methods for exchanging child pornography and communicating with minors. Digital technology and the Internet serve four functions in connection with child pornography and child exploitation: production, communication, distribution, and storage.

19. Computers, tablets and smart/cellular phones ("digital devices") are capable of storing and displaying photographs. The creation of computerized or digital photographs can be accomplished with several methods, including using a "scanner," which is an optical device that can digitize a photograph. Another method is to simply take a photograph using a digital camera or cellular phone with an onboard digital camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names including AGIF@ (Graphic Interchange Format) files, or "JPG/JPEG" (Joint Photographic Experts Group) files.

20. Digital devices are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such computerized movie files, or video files, can be known by several file names including "MPG/MPEG" (Moving Pictures Experts Group) files.

21. The capability of digital devices to store images in digital form makes them an ideal repository for child pornography. A single CD, DVD, or USB thumb drive can store hundreds or thousands of image files and videos. It is not unusual to come across USB thumb drives that are as large as 32GB. The size of hard drives and other storage media that are used in home computers and cellular phones have grown tremendously within the last several years. Hard drives with the capacity of several terabytes are not uncommon. These drives can store hundreds of thousands of images and videos at very high resolution. Tablet devices have average storage capabilities ranging from 4 Gigabytes to 256 Gigabytes. In addition, most tablets have the ability to utilize the various drives (thumb, jump or flash) described above, which can allow a user to access up to an additional 256 Gigabytes of stored data via the tablet. Modern cell phones have average storage capabilities ranging from 4 Gigabytes to 128 Gigabytes. In addition, most cellular phones have the ability to utilize micro SD cards, which can add up to an additional 128 Gigabytes of storage. Media storage devices and cellular phones can easily be concealed and carried on an individual's person. Mobile computing devices, like cellular phones and tablets,

also have the ability to take still and moving images that are easily stored, manipulated or transferred between devices using software or applications installed on each device. Additionally, multiple devices can be synced to a single account and when an image or video file is transferred it can be transferred to all devices synced to the account at the same time. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and to save that image by storing it in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

22. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer or mobile device connected to the Internet, an individual user can make electronic contact with millions of other computer or mobile device users around the world. Many individual computer/mobile device users and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using wired telecommunications lines, wireless signals commonly known as Wi-Fi, and/or cellular service; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers or cellular network; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, Internet Protocol ("IP") addresses[3] and other information both in computer data format and in written record format.

23. These internet-based communication structures are ideal for those seeking to find others who share a sexual interest in children and child pornography, or seeking to exploit children

---

3 The IP address is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range of 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most ISPs control a range of IP addresses. When mobile devices connect to the Internet they are assigned an IP address either by the residential/commercial WiFi ISP or the cellular ISP. The IP address assignments are controlled by the respective provider.

online. Having both open as well as anonymous communication capability allows the user to locate others of similar inclination and still maintain their anonymity. Once contact has been established, it is then possible to send messages and graphic images to other trusted child pornography collectors or to vulnerable children who may not be aware of the user's true identity. Moreover, the child pornography collector need not use large service providers. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other or with children, and to exchange child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired.

24. It is often possible to recover digital or electronic files, or remnants of such files, months or even years after they have been downloaded onto a hard drive or other digital device, deleted, or viewed via the Internet. Such files can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or even years later using readily available forensic tools. When a person "deletes" a file from a digital device, the data contained in the files does not actually disappear; rather the data remains on the device until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, space on a storage medium that is not allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

25. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

26. As is the case with most digital technology, communications by way of computer or mobile devices can be saved or stored on the computer or mobile device used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's

Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

27. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate law enforcement searches. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.

28. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications. Mobile applications, also referred to as "apps," are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game. Examples of such "apps" include LiveMe, KIK messenger service, Snapchat, Meet24, and Instagram. According to Meet24: Meet24 is a free dating service that provides opportunities to see guys and girls online who are ready to chat, find singles nearby and see the distance between you and your friends, send video messages, and exchange photos.

29. Apps have the ability to send notification messages or "push notifications" to the user. The notifications are stored in a short-term queue until either the application has the ability to process it, or the user clears the notification.

V. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

30. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

- Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored,

and it would be generally impossible to accomplish this kind of data search on site; and

- Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

31. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

32. In addition, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2251, 2252, and 2252A, and should all be seized as such.

VI. SEARCH METHODOLOGY TO BE EMPLOYED

33. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- Examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth

herein;

- surveying various files, directories and the individual files they contain;
- opening files in order to determine their contents;
- scanning storage areas;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or
- performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

VII. INVESTIGATION AND PROBABLE CAUSE

34. On February 13, 2020, a detective from the Cherokee County Sheriff's Office (CCSO), outside of Atlanta, Georgia, conducted an online undercover chat posing as a 13 year old female (UC) on the application Meet244. The detective was approached on the Meet24 application by an individual who identified themselves as "Kayla", claiming to be an 18 year old female from Charleston, South Carolina (SUBJECT ACCOUNT 1). The following is an excerpt from the conversation between the UC and SUBJECT ACCOUNT 1:

- SUBJECT ACCOUNT 1: "omgosh... please sit on my face hehe"
- UC: "hey cutie :) i am 13"
- SUBJECT ACCOUNT 1: "Mmmm I don't mind. I'd still eat that pussy out"

Later in the conversation, SUBJECT ACCOUNT 1 sent the UC an image that depicted an adult male erect penis.

35. On February 13, 2020, the CCSO detective obtained a state search warrant for the subscriber information for the SUBJECT ACCOUNT 1 which was served on Meet24. Information provided by Meet24, identified the account as having an account ID of 4287087 and revealed that the account had been accessed utilizing IP address 65.24.236.92 on February 13, 2020. The return information also contained multiple chats between the user of the SUBJECT ACCOUNT 1 and additional Meet24 accounts, in which the SUBJECT ACCOUNT 1 user discussed sexual topics with females who stated that they were underage. A summary of some of those Meet24 conversations follows.

---

4 According to Meet24: Meet24 is a free dating service that provides opportunities to see guys and girls online who are ready to chat, find singles nearby and see the distance between you and your friends, send video messages, and exchange photos.

36. In a chat on February 13, 2020, SUBJECT ACCOUNT 1 and Meet24 account ID 39646042 (VICTIM 1) discussed exchanging images of each other and SUBJECT ACCOUNT 1 performing sexual acts on the user of the account ID 39646042. The following are a few excerpts from the conversation:

- SUBJECT ACCOUNT 1: "Oh! Shoot, I'd wanna full on make out with ya 😊 maybe I'm just crazy"
- VICTIM 1: "Im 14 u?"
- SUBJECT ACCOUNT 1: "Mmm, you're 14? I'd do even more than make out... hehe. I'm 18!"
- VICTIM 1: "Im young"
- SUBJECT ACCOUNT 1: "I dont mind! I still wanna do naughty things to you."

Later in the conversation:

- SUBJECT ACCOUNT 1: "Come onnn, lol! What's your butt like? 😁"
- VICTIM 1: "In school"
- [VICTIM 1 then sends SUBJECT ACCOUNT 1 an image of the back of a young female in a black bikini]
- SUBJECT ACCOUNT 1: "Mmm I definitely wanna grab yours!"
- SUBJECT ACCOUNT 1: "Can I show you something even sexier? □"
- VICTIM 1: "Sure"
- [SUBJECT ACCOUNT 1 then sends VICTIM 1 an image depicting a young female with breast and vagina fully exposed]
- VICTIM 1: "Damn"
- [VICTIM 1 then send SUBJECT ACCOUNT 1 an image of the face of a young female]
- SUBJECT ACCOUNT 1: "You're so cute!! I want you to eat my pussy... then I'll eat yours."
- VICTIM 1: "Though about it before but scared"
- SUBJECT ACCOUNT 1: "Really? You ever had a dick in you before?"

Later in the conversation, they began to discuss SUBJECT ACCOUNT 1's "fuck buddy", who SUBJECT ACCOUNT 1 describes as a 30 year old male. Your affiant believes that the individual SUBJECT ACCOUNT 1 was referencing was Seth Bauman (BAUMAN), identified later as the owner of SUBJECT ACCOUNT 1.

- SUBJECT ACCOUNT 1: "That's a start lol. You need one in that pussy too. I got a fuck buddy who helps me when I need it. Wanna see his?"
- VICTIM 1: "Yea lol"
- SUBJECT ACCOUNT 1: "I like you! Lol, you're fun 😊"
- [SUBJECT ACCOUNT 1 then sends VICTIM 1 the same image of an adult male erect penis that SUBJECT ACCOUNT 1 had sent to the UC, as described above]
- VICTIM 1: "Its long"
- SUBJECT ACCOUNT 1: "Yeah, it's a nice one! You want it in your pussy? I could tell him 😉"

Later in the conversation on the same day:

- SUBJECT ACCOUNT 1: "We're gonna have to make a road trip and come fuck you! Itll be so much fun!"

Later in the conversation on the same day:

- VICTIM 1: "How old is he"
- SUBJECT ACCOUNT 1: "Thank you!! 😊 And he is 30."
- VICTIM 1: "O"
- SUBJECT ACCOUNT 1: "He'll love your 14 yr old tight pussy for sure 😘"
- VICTIM 1: "Hes 30"
- SUBJECT ACCOUNT 1: "Yeah lol"

37. In a chat on February 13, 2020, SUBJECT ACCOUNT 1 and Meet24 account ID 39876694 (VICTIM 2) discuss trading pictures of each other. The following are excerpts of the conversation:

- SUBJECT ACCOUNT 1: "Wanna trade and compare? 😉"
- VICTIM 2: "I don't feel comfortable doing that"
- SUBJECT ACCOUNT 1: "Come on... pleaseee? I'm super horny and that'll be fun!"

Later in the conversation:

- SUBJECT ACCOUNT 1: "I need to see full nude lol, not just that. Would love to see them 15 yr old tits. In turn, you can see my tits and pussy!"
- VICTIM 2: "idk"
- SUBJECT ACCOUNT 1: "Show me how wet you are for now and I'll show you my ass 😋 it's a start lol"
- VICTIM 2: "I will finger u hard and lick your pussy dry"
- SUBJECT ACCOUNT 1: "Mmm that would be so nice right now!"
- [VICTIM 2 then sends SUBJECT ACCOUNT 1 an image of wet panties on the floor]
- VICTIM 2: "there u are"

38. In a chat on February 13, 2020, SUBJECT ACCOUNT 1 and Meet24 account ID 40253877 (VICTIM 3) discuss trading pictures of each other. The following is an excerpt of the conversation:

- SUBJECT ACCOUNT 1: "Mmm, you look so cute and so young!! How old are you really? It'll be our secret □"
- VICTIM 3: "16"
- SUBJECT ACCOUNT 1: "That's hot! I'd so eat your pussy out right now if I could, hehe."
- VICTIM 3: "😊😊😊 please"
- SUBJECT ACCOUNT 1: Mmmm, you got pics of that 16 year old body 😍 I'll

trade some of mine!"

- [SUBJECT ACCOUNT 1 then sends VICTIM 3 an image which depicted a female in orange thong underwear]
- SUBJECT ACCOUNT 1: "You like...?"
- VICTIM 3: "I do!!"
- [VICTIM 3 then sends SUBJECT ACCOUNT 1 an image of a female in purple thong underwear]
- SUBJECT ACCOUNT 1: "I'm glad!! And oh my.. your ass is better than mine lol!"
- [SUBJECT ACCOUNT 1 then sends VICTIM 3 an image of a young female with breast and vagina fully exposed]
- VICTIM 3: "Yours is better"
- [VICTIM 3 then sends SUBJECT ACCOUNT 1 an image of a young female with breast and vagina fully exposed]

39. In a chat on February 13, 2020, SUBJECT ACCOUNT 1 and Meet24 account ID 40288637 (VICTIM 4) discuss trading pictures of each other and performing sexual acts with an adult male who your affiant again believes is BOWMAN. The following are excerpts of the conversation:

- SUBJECT ACCOUNT 1: "You'd probably like my fuck buddy's dick. I know I do 😉"

Later in the conversation, SUBJECT ACCOUNT 1 sent VICTIM 4 the same image of an adult male erect penis that was sent to the UC.

Later in the conversation:

- SUBJECT ACCOUNT 1: "Omg your fun! You need to be here lol. Got any sexy pics of you? I'll show you some of me too. If you want.."
- VICTIM 4: "I don't have any I'm sorry"
- SUBJECT ACCOUNT 1: "That's okay! So are you really 19 or younger? 😉 we dont judge"
- VICTIM 4: "I'm younger"
- SUBJECT ACCOUNT 1: "Mmm, how old?"
- VICTIM 4: "You sure you don't mind"
- SUBJECT ACCOUNT 1: "Yesss, we dont care. It'll be our secret 😘"
- VICTIM 4: "I'm 12"
- SUBJECT ACCOUNT 1: "Omg I'm gonna have to tell him about you. Guarantee he'll want to fuck that pussy."

Later in the conversation:

- SUBJECT ACCOUNT 1: "Show me your tits or pussy babe. I'm really curious! And wet.."

Later in the conversation:

- SUBJECT ACCOUNT 1: "I'd let him fuck me as much as he wants for a day lol. But you gotta show me something good □"
- [VICTIM 4 then sends SUBJECT ACCOUNT 1 an image of a young female with

vagina fully exposed]

- SUBJECT ACCOUNT 1: "Mmmm a little 12 yr old pussy. Such a turn on!"
- VICTIM 4: "Thx"

40. In a chat on February 13, 2020, SUBJECT ACCOUNT 1 and Meet24 account ID 40251257 (VICTIM 5) discuss performing sexual acts with each other as well as trading pictures. The following are excerpts from the conversation:

- SUBJECT ACCOUNT 1: "Omgoodness you're cute! 😊😊 how old are you?"
- VICTIM 5: "17"
- VICTIM 5: "😊"
- SUBJECT ACCOUNT 1: "I freaking love that skirt. Is that a school uniform or something?"
- VICTIM 5: "yes"
- SUBJECT ACCOUNT 1: "You rock it! Lol. Not gonna lie though, wouldnt mind taking it off you either."

Later in the conversation

- [SUBJECT ACCOUNT 1 sends VICTIM 5 an image of a female in orange thong underwear]
- VICTIM 5: "so cute💞💞💞"
- SUBJECT ACCOUNT 1: "Thanks babe! What's your butt like? 😏"
- [VICTIM 5 then sends SUBJECT ACCOUNT 1 an image of a female with vagina fully exposed]

41. On February 24, 2020, the CCSO detective obtained a state search warrant for the subscriber information for the IP address 65.24.236.92, the IP address utilized to access SUBJECT ACCOUNT 1 on the date of all of the above conversations. Responsive information provided by Charter Communications identified the subscriber as Seth BAUMAN, with a physical address of 641 E. Front Street, Apt F5, Logan, Ohio 43138, and phone number 7402749036. At that point, the CCSO detective passed along his case report to Ohio Internet Crimes Against Children (ICAC) task force, and it was subsequently assigned to a Hocking Count Sheriff's Office (HCSO) detective.

42. On February 28, 2020, the CCSO UC conducted an additional online undercover chat again posing as a 13 year old female on Meet24. A Meet24 account, later identified as having account ID 40650191 (SUBJECT ACCOUNT 2), initiated a conversation with the UC. The following are excerpts of the conversation:

- SUBJECT ACCOUNT 2: "Mmm, damn babe, you're so fucking sexy 😍😍 do you like big dick? 😉"
- SUBJECT ACCOUNT 2: "Hope you dont mind me stroking it to your pics..."
- UC: "hey lol. i am 13 lol"

- SUBJECT ACCOUNT 2: "Still sexy 😋 lol. Loving that ass!"

Later in the conversation

- SUBJECT ACCOUNT 2: "Wanna see what I'm stroking..?"
- UC: "sure lol"
- [SUBJECT ACCOUNT 2 then sends UC an image which depicted an adult male erect penis]

43. On March 3, 2020, the CCSO detective sent the HCSO detective the results of a second search warrant that was served on Meet24 for subscriber information related to SUBJECT ACCOUNT 2. The responsive information provided by Meet24 identified the account ID as 40650191 and provided the IP address utilized to access the account as 65.24.236.92. This is the same IP address that was repeatedly used to access SUBJECT ACCOUNT 1.

44. On March 5, 2020, HCSO, along with Ohio ICAC, executed a search warrant on BAUMAN's residence, 641 E. Front Street, Apartment F5, Logan, Ohio 43138. During the search, BAUMAN was read and signed a Miranda Rights waiver, and was interviewed by detectives. The following are excerpts of the statements BAUMAN made during the interview:

- BAUMAN admitted to downloading the MeetEasy app and other dating apps.
- BAUMAN stated he created an account to get on the apps.
- BAUMAN stated that his cell phone is a [Samsung] Galaxy J7.
- BAUMAN admitted to sending pictures of his penis on dating sites before.
- BAUMAN confirmed that when he would send a picture he would get pictures in return.
- When detectives showed BAUMAN images of the adult male with erect penis sent to UC and Victims, BAUMAN confirmed the pictures being of his penis.
- BAUMAN made the statement "Those are my pictures, but I don't want this shit to ruin my life".
- When detectives showed BAUMAN the Meet24 IP address for SUBJECT ACCOUNT 1 and SUBJECT ACCOUNT 2, BAUMAN made the statement "I guess it was me if it is back to my IP address, who else would it be"
- BAUMAN confirmed he has been on the different "meet" apps.

45. At the conclusion of the interviews and execution of the search warrant, BAUMAN was placed under arrest for one count of Pandering Sexually Oriented Material involving a minor and transported to the Southeastern Ohio Regional Jail. Among the items seized during the search warrant was a Black Samsung J7 cell phone SM-S757BL.

46. On March 6, 2020, the HCSO detective reviewed BAUMAN's phone that was seized, a Samsung J7, and identified images 149864334 and 140614029, as described above as images of a female in an orange thong and of an adult male erect penis that the SUBJECT ACCOUNT user sent to other Meet24 users, located on the phone.

47. On March 31, 2020, a search warrant for the devices seized from BAUMAN's residence was signed in the Southern District of Ohio by United States Magistrate Judge Kimberly A. Jolson.

48. During the forensic examination of the Samsung J7, multiple push notifications were observed within the phone's memory. Among the push notifications were several from the Meet24 application. One push notification related to a message from Victim 2 sent on February 13, 2020 to SUBJECT ACCOUNT 1, indicating that the Samsung J7 phone was used to receive chats from Victim 2, and that SUBJECT ACCOUNT 1 was logged into the Meet24 app on the phone. Additionally, another push notification related to a message from the UC sent on February 28, 2020 to SUBJECT ACCOUNT 2, indicating that SUBJECT ACCOUNT 2 was logged into the Meet24 app on the phone.

49. Continued review of the Samsung J7 push notifications revealed additional push notifications sent from Meet24 accounts that did not relate to the two previously identified Meet24 accounts. This would indicate that there were other accounts logged into the phone besides SUBJECT ACCOUNTs 1 and 2.

50. Based on the information that BAUMAN was the owner and user of the Samsung J7, that both SUBJECT ACCOUNTs 1 and 2 were logged into BAUMAN's phone, both SUBJECT ACCOUNTs 1 and 2 were registered from IP Address 65.24.236.92, the sexual content of the chats and images sent on Meet24 from both SUBJECT ACCOUNTs 1 and 2, and the evidence of push notifications sent to additional accounts on the Samsung J7 other than SUBJECT ACCOUNTs 1 and 2, your affiant has reason to believe that the contents of the additional ACCOUNTS are likely to contain communications and images which may constitute contraband and evidence of criminal violations of 18 U.S.C. §§ 2251, 2252(a), 2252A, and 2422(b).

VIII. CHILD SEXUAL EXPLOITATION OFFENDER CHARACTERISTICS

51. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals who produce, distribute, and receive child pornography as well as those who communicate online with

other subjects about the sexual abuse of children:

- Those who communicate about and engage in online sexual abuse of children and exchange or collect child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
- Those who communicate about and engage in online sexual abuse of children and exchange or collect child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- Those who communicate about and engage in online sexual abuse of children and exchange or collect child pornography often times possess and maintain any "hard copies" of child pornographic material that may exist B that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and video tapes for many years.
- Likewise, those who communicate about and engage in online sexual abuse of children and exchange or collect child pornography often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.
- Those who communicate about and engage in online sexual abuse of children and exchange or collect child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as

they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

- Those who communicate about and engage in online sexual abuse of children and exchange or collect child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography offenders throughout the world.
- When images and videos of child pornography are produced and stored on computers and related digital media, forensic evidence of the production, distribution, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media.

52. Based upon the conduct of individuals involved who communicate about and engage in online sexual abuse of children and exchange or collect child pornography set forth in the above paragraphs, namely, that they tend to maintain their collections at a secure, private location for long periods of time, and that forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media, there is probable cause to believe that evidence of the offenses of production, distribution and possession of child pornography is currently located on the **ACCOUNTS**.

IX. CONCLUSION

53. Based on the aforementioned factual information, your affiant submits there is probable cause to believe that violations of Title 18, United States Code, Sections 2252, 2252A, 2251, and 2422 have been committed, and evidence of those violations is located on the **ACCOUNTS** described in Attachment A, and on any computers or computer related media found within. Your affiant respectfully requests that the Court issue a search warrant authorizing the search and seizure of the items described in Attachment A.

Josh Saltar

Special Agent

Federal Bureau of Investigation

Sworn to and subscribed before me this 8th day of May, 2020.

Elizabeth A. Preston Deavers
United States Magistrate Judge

ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant applies to information associated with all Meet24 accounts with the Registration IP Address 65.24.236.92 that is stored at premises owned, maintained, controlled, or operated by Wildec LLC, a company headquartered in Everett, Washington.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

I. Information to be disclosed by Wildec LLC

To the extent that the information described in Attachment A is within the possession, custody, or control of Wildec LLC ("Wildec"), regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Wildec, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Wildec is required to disclose the following information to the government for each account with the Registration IP listed in Attachment A:

a) All contact and personal identifying information, including: full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

b) All photos and videos uploaded or received by the user, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;

c) All profile information, location information, activity logs, and all other records and contents of communications and messages made or received by the user;

d) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;

e) All IP logs, including all records of the IP addresses that logged into the account;

f) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

g) All records pertaining to communications between Wildec and any person regarding the user or the user's account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2252, 2252A, 2251, and 2422 involving the accounts of the user(s) with Registration IP address identified on Attachment A, information pertaining to the following matters:

(a) Any and all communications related the production, receipt, distribution or possession of child pornography; and to persuade, induce, entice, or coerce or attempt to persuade, induce, entice or coerce, any individual who has not attained the age of 18 years, to engage in any sexual activity for which any person may be charged with a crime, including the production of child pornography;

(b) Evidence indicating how and when the Meet24 account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Meet24 account owner;

(c) Evidence indicating the Meet24 account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

Wildec is hereby ordered to disclose the above information to the government within 10 days of service of this warrant.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.